Department of Homeland Security Daily Open Source Infrastructure Report for 07 December 2005

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Immigration and Customs Enforcement special agents on Thursday, December 1, carried out enforcement actions resulting in the arrest of aliens who were illegally working at Kirtland Air Force Base in Albuquerque, New Mexico. (See item 3)
- The U.S. Department of Health and Human Services on Monday, December 5, convened senior state and local officials to establish an integrated federal−state influenza−pandemic planning process. (See item 22)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *December 06, Energy Information Administration* — **Short term energy forecast released.** According to the Energy Information Administration, sharp increases in energy prices and hurricane−related supply losses in oil and natural gas dominated the news in U.S. energy markets in 2005. While demand generally drove 2004 energy prices higher, in 2005 the price increases were more the result of supply concerns because of the hurricane losses, as well as the reduction in world oil spare capacity, which fell to its lowest level in over three decades. As U.S. spot prices of crude oil and natural gas increased an average of 36 and 47 percent, respectively, total U.S. energy demand remained flat this year, despite a relatively healthy

economic growth rate of more than three percent. Similarly, world oil prices climbed throughout the year despite slower demand growth in both China and the United States. In 2006, total domestic energy demand is projected to increase at an annual rate of about two percent, despite continued concerns about tight supplies and projected high prices for oil and natural gas.
Short term energy outlook: http://www.eia.doe.gov/emeu/steo/pub/dec05.pdf
Source: http://www.eia.doe.gov/steo

2. *December 05, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission and states issue requirements for increased controls on certain radioactive materials.** The Nuclear Regulatory Commission (NRC) and state regulators have issued legally binding requirements to licensees to implement increased controls over radioactive materials in certain "quantities of concern." The requirements are the first part of a cooperative effort, announced in September, between the NRC and the 33 Agreement States to enhance controls of radioactive materials that could potentially be of use to terrorists. The NRC's Order to its licensees was published December 1 in the Federal Register. As of December 2, the Agreement States have issued the increased controls to their licensees. Approximately 2,200 licensees nationwide have received the requirements. Agreement States are those that regulate the medical, industrial and academic uses of radioactive materials under agreements with the NRC.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2005/05−1 64.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *December 02, Immigration and Customs Enforcement* — **Illegal aliens arrested at military base.** Immigration and Customs Enforcement (ICE) special agents on Thursday, December 1, carried out an enforcement actions resulting in the arrest of aliens who were illegally working at a military base in New Mexico. ICE special agents teamed up with the Air Force Office of Special Investigation (OSI) and base Military Police to arrest 22 Mexican nationals who were illegally working for one of six subcontractors on a housing project at Kirtland Air Force Base (AFB) in Albuquerque, NM. The individuals were arrested following a document check at the military installation. ICE first began checking documents at Kirtland AFB after receiving information from OSI and the U.S. Border Patrol about illegal aliens who were recently arrested trying to enter the Department of Defense and the Department of Energy installation. "Removing illegal aliens from sensitive worksites is a top priority for ICE," said Kyle Hutchins, special agent−in−charge of the ICE El Paso Office of Investigations. "By removing unauthorized workers from critical infrastructure sites, such as U.S. military installations, we're shutting down significant vulnerabilities and potential threats to the security of our homeland," said Hutchins.
Source: http://www.ice.gov/graphics/news/newsreleases/articles/05120 2washington.htm

[Return to top]

Banking and Finance Sector

4. *December 06, IT Observer* — **Hackers steal sensitive data using digital cameras.** Following a spate of reports about Bluetooth and iPods devices being used to steal sensitive data from organizations, businesses are now urged to be vigilant as hackers use digital cameras to sidestep security measures. “Camsnuffling,” is being used by computer attackers to extract and store data with the help of digital camera. The digital camera device, just like iPod and Bluetooth, is a simple digital storage device. Hence, simply plugging it into a computer’s USB can allow hackers to obtain sensitive data. "This is a very difficult issue to manage and a real threat to business continuity and data security,” according Ian Callens, of computer services company Icomm Technologies. "There are, however, steps that can be taken to reduce rogue behavior," said Callens. "Firstly, regularly change system passwords that employ both letters and numerals. Secondly, issue internal memo’s to ask all to be vigilant, stating that observations are being undertaken. Thirdly, consider adopting specific software to monitor activity to actively manage the access rights to removable storage devices. This should ensure that business productivity is not affected, while actively guarding against the removal of data or the introduction of inappropriate or malicious content to the network," said Callens.
Source: http://www.ebcvg.com/articles.php?id=966

5. *December 06, Nbc4i.com (OH)* — **Women arrested in alleged counterfeit ring.** Police in Westerville, OH, said Monday, December 5, that they tipped off Tennessee authorities to two women when they stumbled upon a fake check. Georgina McGill and Candy Roberts, both of Columbus, OH, were arrested in Nashville on Thursday, December 1, and are being called alleged key players in a counterfeit check ring. On Friday, December 2, police searched the homes of both women, looking for fake identifications and stolen checks. Authorities said the women traveled from Columbus on a regular basis to Nashville, Memphis and into Georgia, cashing in the fake payroll checks. "We don't know if there are any individual victims out there but we know several financial institutions have been targeted by these individuals," said Westerville police detective Ted Smith. Police said the women raked in nearly $60,000 each week and said evidence found in their homes suggests more arrests are on the way.
Source: http://www.nbc4i.com/news/5476034/detail.html?rss=col&psp=ne ws

6. *December 05, IDG News Service* — **Ebay tricked by phony e−mail.** A sophisticated phishing attack has proven to be so successful, it has tricked eBay Inc.'s own fraud investigations team into endorsing it as legitimate, according to an independent security consultant who reported the attack to eBay. In late November, Richi Jennings received a fraudulent e−mail message containing the subject line "Christmas is Coming on ebay.co.uk." Offering him "great tips for successful Christmas selling," the message directed him a Website that asked Jennings to enter his eBay user name and password, as well as the name and password for his e−mail account. Jennings reported the site to eBay on November 25, and four days later he got a note back from the company's investigations team claiming that the e−mail message was, in fact, "an official e−mail message sent to you on behalf of eBay." On Monday, December 5, eBay spokesperson Amanda Pires confirmed that the e−mail message was indeed part of a fraud, but she could not explain why it had initially been identified as legitimate. Pires said that eBay had been working

to take down the phishing site since November 8.
Source: http://www.infoworld.com/article/05/12/05/HNebaytricked_1.ht ml

[Return to top]

Transportation and Border Security Sector

7. *December 06, USA TODAY* — **Airlines cram more fliers into fewer seats, flights.** For the first time in recent aviation history, the financially troubled U.S. airline industry is shrinking domestic flying capacity in the face of strongly growing public demand for its service. For consumers, diminished capacity could mean higher average fares, fewer choices, fuller flights and fruitless searches for mileage upgrades and award travel. For communities, it could mean deteriorating or disappearing air service. For the airlines themselves, it could mean a fighting chance to regain profitability. A USA TODAY analysis shows that the number of scheduled domestic airline seats this month will fall five percent below last year. It means that 3.9 million airline seats offered for sale last December aren't there this year. That's an average of 126,000 seats per day. Meanwhile, the number of air travelers has been growing strongly since the September 11 attacks. The Federal Aviation Administration projects 19 percent more domestic air passengers in 2006 than traveled in 2002. For some carriers, the cutbacks are "a matter of survival," says John Heimlich, economist for the Air Transport Association. Capacity reduction cuts expenses and improves airlines' pricing power by constricting the supply of airline seats.
Source: http://www.usatoday.com/travel/news/2005−12−06−air−capacity_x.htm

8. *December 06, Canadian Press* — **Canadian train car loaded with autos crashes into river.** A CN Rail train has derailed on a trestle crossing the Fraser River between Richmond and Burnaby, British Columbia, sending a railcar loaded with automobiles into the Fraser River on Monday, December 5. The derailment was the second of the day for CN, after seven empty cars jumped the tracks in the Cheakamus Canyon north of Squamish, British Columbia. A stretch of the Vancouver−area bridge's railing was snapped off where the car carrier plunged into the water. The derailed rail cars impeded some traffic on the Fraser River. There was no indication of anything toxic spilling into the river, said a CN spokesperson, although some gasoline from the automobiles may have leaked. CN has staunchly defended its safety performance, arguing that despite privatization and job cuts, new monitoring technology has made it the safest railway in North America.
Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&pubid=968163964505&cid=1133867934061&col=968705899037&call_page=TS_World&call_pageid=968332188854&call_pagepath=News/World

9. *December 06, Canadian Press* — **Thousands of Ontario licenses, permits missing.** Thousands of license plates and permits have gone missing or were stolen, the province's auditor general found in his 2005 report released on Tuesday, December 6. Staff at the 280 private licensing operations across the province are creating fake driver's licenses, a key piece of identification used to obtain other vital documents such as birth certificates and passports, and are misusing people's credit card information, the auditor general Jim McCarter found. In the past four years, 56,000 license plates, temporary driver's licenses and permits have gone missing −− 7,000 of which were reported stolen −− from private licensing operations and could

have been used for illegal purposes, the report says. The private network of offices handles about 80 percent of the province's vehicle registrations and 40 per cent of its driver−license transactions. It's allowing people to use membership cards from wholesale warehouse retailers, such as Price Club or Costco, and student cards −− even if they don't include a picture −− as a valid piece of identification to get a license. "We concluded that the ministry needs to strengthen its systems and procedures if it is to ensure that only legitimate and safe drivers are licensed to drive in Ontario," the report says.
Source: http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1133867934072&call_pageid=968332188492&col=968793972154

10. *December 06, Reuters* — **CFO: JetBlue looking for cost cuts, revenue hikes.** JetBlue Airways is looking to cut costs as it seeks to recover from its first loss−making year since going public in April 2002, the carrier's chief financial officer said Tuesday, December 6. At the same time the No. 3 U.S. airline by market value is looking for new ways to boost revenue as it pushes forward with an aggressive expansion plan, CFO John Owen told the Reuters Aerospace and Defense Summit. On the cost side, the airline has taken steps including selective flight cutbacks on routes which are less profitable at currently high fuel prices and further automating some functions. Still, he acknowledged in a phone interview with the summit, held in Washington, that there is not a lot of fat to cut at the already lean airline. "We take cost control around here very seriously," he said.
Source: http://www.usatoday.com/travel/news/2005−12−06−jet−blue_x.ht m

11. *December 05, Reuters* — **EU ministers give nod to airline blacklist.** European Union (EU) governments gave the go−ahead on Monday, December 5, to the establishment of a blacklist of airlines that are considered too unsafe to fly within the 25−nation EU. Transport ministers meeting in Brussels approved the proposal, which the European Parliament supported last month. The new rules are set to come into force at the beginning of 2006, creating a legal basis for a common EU list of banned carriers. EU member states will tell the executive European Commission which airlines are prohibited from operating on their territory. Then the Commission will draw up the blacklist, based on common criteria. France, Belgium, and Britain have already published lists of companies grounded due to poor safety records. But an airline banned in one EU state can still land in a neighboring country.
Source: http://www.usatoday.com/travel/news/2005−12−05−airline−black list_x.htm

[Return to top]

Postal and Shipping Sector

12. *December 06, Associated Press* — **United States Postal Service climbs out of debt.** The U.S. Postal Service (USPS) is debt free, but even a projected surplus won't stop next month's postal rate increase, which the service says is needed to cover a congressionally mandated expense. On January 8, 2006, USPS plans to raise the price of a first−class stamp to 39 cents and other rates will rise accordingly. Once $11 billion in the red, the post office paid off the remaining $1.8 billion of its debt in 2005, postal Chief Financial Officer Richard Strasser said Tuesday, December 6. It's the first time the Postal Service has been without debt since it was organized from the old post office in the 1970s.

Source: http://www.latimes.com/news/nationworld/politics/wire/sns−ap−postal−finances,1,3480770.story?coll=sns−ap−politics−headli nes

[Return to top]

Agriculture Sector

13. *December 05, Agriculture Online* — **Elk may test animal identification system in Texas.** Elk in Texas will have radio frequency identification (RFID) ear tags beginning after the first of the year if the Texas Animal Health Commission (TAHC) adopts proposed disease control tracking regulations. "Identification and record keeping requirements will be extremely useful for quickly tracing elk movements, if chronic wasting disease (CWD)- or other diseases, such as brucellosis or tuberculosis are detected in the animals," said Bob Hillman, executive director for the TAHC.
Source: http://www.agriculture.com/ag/story.jhtml?storyid=/templated ata/ag/story/data/1133797406573.xml&catref=ag1001

14. *December 05, Western Farm Press* — **Mustard cover crops tested for lettuce disease control.** Mustard cover crops appear to be a positive cultural practice and should be evaluated for their potential as a means of reducing lettuce head drop disease and weeds in coastal California counties. That is the conclusion of Richard Smith, Monterey, CA, farm advisor, after a series of trials with commercial varieties of white and Indian mustard species planted as covers between lettuce crops. Smith said lettuce drop, caused by the fungus, Sclerotinia minor, is the primary soil borne disease of lettuce in the Salinas Valley. There has been a flurry of interest among growers in the valley in mustard crops as a cover crop to provide control of head drop and weeds. Many research projects around the world, Smith noted, have shown mustards develop glucosinolate compounds that are antagonistic to disease and weed pests. In detailing his final results from the Indian and white mustard trials, Smith said they have “a slight but significant impact on Sclerotinia.” He also saw some disease reduction with covers of Merced rye used as a comparison. All the cover crop plots (including the two mustards and Merced rye) for 2004 and 2005 showed improved head weight yields over the fallow, untreated check plots.
Source: http://westernfarmpress.com/news/12−5−05−mustard−cover−crops /

[Return to top]

Food Sector

15. *December 06, Korea Herald (South Korea)* — **Decision due on lifting U.S. beef ban.** A panel of livestock experts will convene the week December 12 for a meeting expected to be key in South Korea's decision to finally lift its ban on U.S. beef imports. According to the Ministry of Agriculture and Forestry, the livestock quarantine committee meeting will cover safety issues concerning U.S. beef and countermeasures for cattle ranchers in South Korea. The 17−member committee, comprised of government officials, veterinarians, consumer groups, and cattle ranchers, failed to reach a consensus on whether to lift the ban at their last meeting on November 29, pushing them to postpone their proposal by another two weeks. Meat producers and consumer groups are strongly opposed to Seoul lifting the ban. But the Korean government

says that as long as U.S. beef is safe to consume, it should no longer delay the imports any longer. South Korea banned U.S. beef in December 2003 after a case of mad cow disease was discovered the state of Washington.
Source: http://www.koreaherald.co.kr/SITE/data/html_dir/2005/12/07/2 00512070016.asp

16. *December 05, Dow Jones* — **Bovine spongiform encephalopathy tests on healthy looking cattle completed.** The U.S. Department of Agriculture (USDA) has completed mad cow disease testing program on cattle that appeared completely healthy and found no positive cases, a USDA official said Monday, December 5. USDA's goal was to test 20,000 healthy looking cattle, but the department stopped after 21,216 were tested. Ron DeHaven, head of USDA's Animal and Plant Health Inspection Service, said the tests were not meant to have "any statistical significance," but were solely intended to "keep the testing system honest." Most of the cattle USDA has tested for mad cow disease, or bovine spongiform encephalopathy, are considered to be in a higher risk category for the disease. Those higher risk cattle are, for example, animals that are too sick or injured to walk or animals that are dead on arrival at processing plants.
Source: http://www.cattlenetwork.com/content.asp?contentid=14543

[Return to top]

Water Sector

17. *December 06, MosNews* — **Two Britons detained in Azerbaijan on suspicion of bioterrorism.** Police in Baku, the capital of the former Soviet republic of Azerbaijan, have detained two British nationals near a water reservoir under suspicion of trying to poison water supplies. The two men were arrested on Saturday, December 3, as they were trying to pour a white powder into the water. The powder has been sent for examination. Preliminary reports identified the suspects as Paul Williamson and Duncan Jackson, employees of British Petroleum. The Azeri police said a map of the area was found on the detainees. The expatriates were questioned at the district police department for several hours but did not explain why they had entered the area of the water reservoir. The National Security Ministry is currently investigating.
Source: http://www.mosnews.com/news/2005/12/06/bakuarrest.shtml

18. *December 06, Arizona State University* — **Invention speeds up bacteria identification.** Arizona State University (ASU) researchers have invented a sensor that could play an important role in early detection of disease−causing bacteria or bioterrorism agents in drinking water supplies. The researchers unveiled their invention Monday, December 5, at the Arizona Water Quality Center's (WQC) meeting. Developed by WQC Director Morteza Abbaszadegan and his ASU research team, the biosensor uses fiber optics, wireless communication, and a chemical process to identify bacteria in 10 minutes. Identifying those same bacteria usually takes between 24 and 48 hours using current methods. Abbaszadegan said, "We have developed bacterial signatures...By knowing those signatures, we can identify bacteria in an unknown sample." In the case of disease−causing bacteria, identifying unsafe drinking water needs to be done quickly. Binga Talabi, senior chemist for the Scottsdale water quality department, said a device like the biosensor could improve any city's preparedness in the event of a bioterrorism attack. "The focus of most municipalities is to find real−time monitoring systems like this," he

said. In addition to the device's speed, another advantage is that it could be installed onsite, enabling more accurate readings, said research associate Mohamad Elzein. Abbaszadegan said the biosensor could also be adapted to detect hormones in water sources.
Source: http://www.asuwebdevil.com/issues/2005/12/06/news/695233

19. *December 06, Pasadena Star News (CA)* — **National Aeronautics and Space Administration agrees to pay for groundwater cleanup at Jet Propulsion Laboratory site.** The National Aeronautics and Space Administration (NASA), which operates the Jet Propulsion Laboratory in La Canada Flintridge near Pasadena, CA, has agreed to build a water treatment plant to remove the toxic chemical perchlorate from four Pasadena−owned wells, with construction to begin sometime in 2007. The agreement comes eight years after perchlorate was first detected in the Monk Hill aquifer, and follows several years of intensive negotiations in which city officials pressed NASA to take responsibility for the contamination and pay to treat the local groundwater. Pasadena has had to close nine wells in all because of perchlorate contamination. City officials hope the agreement signals a willingness on NASA's part to pay for cleanup perchlorate contamination at a second site, the Sunset basin, where five additional wells have been taken out of service. Perchlorate has been shown to disrupt normal thyroid function. According to the agreement, NASA will spend up to $4.9 million to design and build a water treatment facility over the Monk Hill basin, where the four wells are located.
Source: http://www.pasadenastarnews.com/news/ci_3282456

[Return to top]

Public Health Sector

20. *December 06, Xinhua (China)* — **China confirms new human case of bird flu.** The China Ministry of Health (MOH) on Tuesday, December 6, confirmed a new case of human infection of bird flu in Ziyuan County of south China's Guangxi Zhuang Autonomous Region. The patient is a 10−year−old girl, who has been ill with fever and pneumonia since November 23, said an MOH press release. The girl tested positive with the H5N1 virus by the China Disease Prevention and Control Center, and she has been under emergency treatment in a hospital. People who have close contacts with the patient have been brought under medical observation by local health departments. So far, no abnormities have been found among these people. The regional health department and MOH have sent expert teams to direct and coordinate disease prevention and control in the area. Currently, experts are making further investigation in the source of the bird flu virus, since no bird flu cases have been reported in the county before.
Source: http://news.xinhuanet.com/english/2005−12/06/content_3885831 .htm

21. *December 05, ComputerWorld* — **Two New York hospitals launch patient smart−card initiative.** Two major hospitals in the New York metropolitan area have joined with a vendor of smart−card technologies on a pilot project designed to provide patients with better portability of their health care information and give doctors better access to that data. Under the initiative announced Monda, December 5, Mount Sinai Medical Center and the Elmhurst Hospital Center will initially deploy around 100,000 smart cards to patients at the two hospitals and several other affiliates in the area beginning in the second quarter of 2006. Each institution will issue smart cards that integrate the patient's identity data with essential health information that can be quickly accessed and routinely updated by health care professionals who are part of the regional

smart−card network. Eventually, 45 affiliated and related health care facilities in the area will be linked by the smart−card initiative. "Right now, there's a lot of interest to create a national hospital network" that would make health care information more broadly accessible to providers and patients, said Jack Nelson, CIO at Mount Sinai. The smart−card initiative is one way of making such information portable without investing in the infrastructure needed for a connected health care network, he said.
Source: http://www.computerworld.com/databasetopics/data/story/0,10801,106773,00.html?source=NLT_PM&nid=106773

22. *December 05, U.S. Department of Health and Human Services* — **Federal government begins pandemic planning with states.** U.S. Department of Health and Human Services (HHS) Secretary Mike Leavitt Monday, December 5, convened senior state and local officials to establish an integrated federal−state influenza−pandemic planning process. Officials from every U.S. state, territory, Puerto Rico, and tribal governments participated. The officials were advised to plan broadly. Leavitt asked participants to begin preparing for a series of in−state pandemic−planning summits to be held in every state over the next several months. These in−state summits will help the public health and emergency response community in each state inform and involve their political, economic, and community leadership in this process. The first local meeting will be held jointly with Governor Tim Pawlenty in Minneapolis, MN, on December 14. HHS advised states to establish a Pandemic Influenza Coordinating Committee to draft and adopt a plan that will delineate the roles and responsibilities of state and local agencies and offices; build on existing preparedness and response plans for bioterrorism events and infectious disease emergencies; address legal issues including those that affect hospital staffing, patient care and quarantine; and be periodically reviewed and updated. Leavitt issued a checklist which summarizes key planning activities to be undertaken by the public health system of each state in collaboration with partners.
Checklist: http://www.pandemicflu.gov/plan/statelocalchecklist.html
Source: http://www.hhs.gov/news/press/2005pres/20051205.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

23. *December 06, Stars and Stripes* — **Terminal Fury will test teamwork in the Pacific.** Military personnel in Japan and Hawaii are conducting a two−week exercise this month to test their ability to come together and regroup as a joint task force to manage emergencies in the region. Terminal Fury '06 is a command post exercise −− a simulation rather than training in the field −− held both in Hawaii and aboard the USS Blue Ridge based at Yokosuka Naval Base, Japan. The exercise tests the abilities of the Pacific Command and Joint Task Force 519, a group created several years ago to respond quickly to emergencies in the Pacific Command area of responsibility. The task force is joint, meaning it includes all services. It is designed to be

deployable aboard a ship and capable of command and control of Pacific and stateside assets in a war or natural disaster. Terminal Fury will run for the first two weeks of December. The key objectives of the exercise are to exercise, evaluate, and improve joint coordination, procedures, plans, and systems necessary for conducting contingency operations on little or no notice.
Source: http://www.estripes.com/article.asp?section=104&article=3348 3

24. *December 06, 10 News Now (NY)* — **State Preparedness Center announced in New York.** Monday, December 5, New York Governor Pataki announced the site for the nation's first State Preparedness Center: Mowhawk Valley in Oneida County, NY. "This facility is virtually ready to go here in Oneida County airport. It has the classroom space. It has the office space that we need and the capital investment will not be that great. We also wanted a place where you could get in and out of very easily and the transportation access here is tremendous," said Pataki. The facility will serve as the hub for emergency response training for natural, technological, and terrorism related disasters. There are also plans for a new emergency operations center at the site. Pataki says the Mohawk Valley's centralized location and proximity to Rome lab make it a suitable location. "We want to make this a national model for how you train first responders," said Pataki. Training at the facility is scheduled to begin by the middle of next year. Pataki says it's expected five to six hundred trainees may come through the facility at any one time.
Source: http://news10now.com/content/all_news/?ArID=54993&SecID=83

25. *December 06, Newsday (NY)* — **In New York City, communication issues fixed.** Police and firefighters can communicate during emergencies in New York City, officials said Monday, December 5, as a federal report decried the lack of such communications on a national level. The city came under strong criticism following the September 11, 2001, terrorist attacks for a variety of communications problems. Some of those were local, such as the use of outdated hand−radios, but other problems were common to most cities and states. One of the most nettlesome of those widespread problems was the lack of interoperability. The city has insisted for some time that it has solved that problem and has conducted joint agency drills at which the agencies had no trouble talking. "There are communication channels that exist that provide communications interoperability between the Fire Department and Police Department," the New York Fire Department said in a statement Monday. "They've been tested. They work, and protocols are in place for their use," the statement said.
Source: http://www.newsday.com/news/local/longisland/ny−liradi1206,0 ,4930314.story?coll=ny−top−headlines

26. *December 05, Government Technology* — **License plate reader alerts trooper to kidnapping suspects.** A new technology called the Automatic License Plate Recognition (ALPR) system is in the first week of a test by the Pennsylvania State Police. Motorola Inc. and PIPS Technology are releasing it to public safety organizations nationwide. The technology installed in police cars "reads" vehicle plates as they enter the view of a vehicle−mounted or roadside infrared camera, and checks them against a database for nearly instantaneous identification. The system runs continuously, automatically capturing images of license plates with a camera that works in nearly every lighting condition. Previous technologies required officers to manually type in a plate number and request a database search for each number, which can be time consuming and prone to errors. In addition to the public safety applications for ALPR, parking garage operators can use the system to control access to their properties and help prevent fraud. Each customer designs its own database to ensure the plates are checked for the type of violators being sought.

In addition to improving security for any type of user, the ALPR system also can help generate revenue by identifying plates with outstanding traffic tickets and overdue parking lot fees.
Source: http://www.govtech.net/news/news.php?id=97445

[Return to top]

Information Technology and Telecommunications Sector

27. *December 05, eWeek* — **Two years later, Blaster Worm still thriving.** More than two years after the Blaster Worm proliferated, the worm is still very much alive and there are fears within Microsoft that thousands of Windows machines will never be completely dewormed. According to statistics culled from Microsoft's Windows malicious software removal tool, between 500 and 800 copies of Blaster are removed from Windows machines per day. "The continued prevalence of [Blaster] is likely due to infected computers which, for one reason or another, will never be updated or disinfected. These computers will serve as eternal carriers for the worm," says Matthew Braverman, a program manager in Microsoft's Anti−Malware Engineering Team. In a case study on Blaster presented to the Virus Bulletin conference in October, Braverman said Blaster ranked in the top five of the most prevalent worms removed by the anti−malware utility. Braverman said the worm continues to be prevalent on a whopping 79 percent all Windows XP (Gold) machines and 21 percent of all Windows XP SP1 systems. On Windows XP SP2, infections are almost nonexistent, Braverman said, pointing out that XP SP2 systems went through a major post−Blaster security overhaul that means those systems cannot be infected through Blaster's main replication vector.
Source: http://www.eweek.com/article2/0,1895,1896373,00.asp

28. *December 05, eWeek* — **Flaw found in Microsoft's SQL Server 2000 Profiler.** A recently discovered vulnerability in Microsoft Corp.'s SQL Server 2000 database allows users to mask their login names. The vulnerability was discovered by Imperva, a researcher and vendor of data−center security products. The flaw shows up in the use of SQL Profiler in Microsoft SQL Server 2000 to audit connections to SQL Server 2000 by using the Audit Login event class. When login names contain leading zero characters, those names are not visible in the contexts of the SQL Profiler graphical user interface, a trace file that is saved by SQL Profiler, and in a trace table that is saved by SQL Profiler. Microsoft put out an advisory that stated that the problem only applies to the Profiler in SQL Server 2000. The problem is fixed in the Profiler in SQL Server 2005 when users use the Profiler to audit connections to SQL Server 2005. Microsoft recommends that users audit connections to SQL Server 2000 by using server−side tracing and by loading the resulting data from a server−side trace file into a database table by using the fn_trace_gettable function.
Microsoft Advisory: http://support.microsoft.com/default.aspx?scid=kb;en−us;9107 41
Source: http://www.eweek.com/article2/0,1895,1896302,00.asp

29. *December 04, SecuriTeam* — **Zone Labs ShowHTMLDialog bypassing vulnerability.** Zone Alarm products with Advance Program Control or OS Firewall Technology enabled, detects and blocks almost all those APIs (like Shell, ShellExecuteEx, SetWindowText, SetDlgItem etc) which are commonly used by malicious programs to send data via http by piggybacking over other trusted programs. By exploiting Zone Lab's trust in certain Web−based programs, malicious programs can bypass Zone Alarm Pro and Internet Security Suite protection and send

information about the system to attackers.
Source: http://www.securiteam.com/windowsntfocus/6N00115EUS.html

30. *December 04, IDG News Service* — **Analysis: Sony rootkit problem raises questions for security vendors.** Sony BMG Music Entertainment has been lambasted for shipping its spywarelike XCP software on music CDs over the past year, but an important question has gone largely unanswered: Why didn't security vendors catch the problem sooner? Though one security vendor, Finland's F−Secure Corp., was aware of the problems surrounding Extended Copy Protection (XCP), none of the major anti−spyware or antivirus vendors had any idea that something was amiss, according to representatives from Symantec Corp., McAfee Inc., and Computer Associates International Inc. There were two things about XCP that presented challenges for the big security vendors. The first was Sony's use of rootkit techniques to cloak XCP and make it harder to circumvent its copy−protection capabilities. A second problem is that the software was distributed by a trusted company: Sony. Sony has sold an estimated two million CDs containing the copy−protection software, which used special rootkit techniques to hide itself on PCs. Rootkit software runs at a very low level of the operating system and is designed to be extremely difficult to detect. Ultimately, XCP's cloaking ability was used by hackers to write malicious software, a development that prompted Sony to recall its XCP CDs.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,106759,00.html

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles requests to the window() object. If exploited, the vulnerability could allow a remote attacker to execute arbitrary code with the privileges of the user. Additionally, the attacker could also cause IE (or the program using the WebBrowser control) to crash. US−CERT strongly encourages Windows users to disable Active Scripting please see:
https://www.cert.org/tech_tips/malicious_code_FAQ.html#ie56

According to Microsoft, malicious software is targeting this vulnerability. We have confirmed that the proof of concept code is successful on Windows 2000 and Windows XP systems that are fully patched as of November 30, 2005.

For more information about this vulnerability please review URL: VU#887861
http://www.kb.cert.org/vuls/id/887861

Reports of IRS Phishing Emails: US−CERT has received reports of a phishing email scam that attempts to convince the user that it is from the Internal Revenue Service (IRS) by using a spoofed "From" address of "tax−refunds@irs.gov".

For additional information on ways to avoid phishing email attacks, US−CERT recommends that all users review the following:
Avoiding Social Engineering and Phishing Attacks at URL:
http://www.us−cert.gov/cas/tips/ST04−014.html

Spoofed/Forged Email at URL: http://www.cert.org/tech_tips/email_spoofing.html

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 139 (netbios−ssn), 1025 (win−rpc), 554 (rtsp), 2745 (Bagle.C), 1434 (ms−sql−m), 1433 (ms−sql−s), 4899 (radmin), 1026 (win−rpc) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

31. *December 06, Associated Press* — **Exploding pens injure three at California schools.** Booby−trapped pens exploded and injured three people at local high schools, causing minor burns and scratches on their hands and faces. The pens were found lying on the ground and blew up when people pulled off their caps. The most recent case was Friday, December 2, when a marker pen exploded in a boy's hands at El Monte High School in El Monte, CA. Detective Gary Spencer of the Los Angeles County Sheriff's bomb squad believes the devices are homemade. School administrators have warned students about picking up objects, said El Monte High Principal Joel Kyne
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−exploding−pens,0,6264423.story?coll=sns−ap−nation−headlines

[Return to top]

General Sector

32. *December 06, Agence France−Presse* — **Military plane crashes in Tehran; 119 killed.** An Iranian military C−130 transport plane crashed into a 10−story apartment building on Tuesday, December 6, killing 119 people, including 25 on the ground, state media and officials said. The building was reported to be on fire, and fire fighters were on the scene working to save people trapped in the building in the Azari residential district. State television said the plane encountered a "technical problem" immediately after take−off from Tehran's Mehrabad airport, which handles domestic, international, and military flights. It said there were 94 people −− 10 crew and 84 passengers −− on board the flight, which was heading for the southern port city of Bandar Abbas. Iran's air force is believed to have no more than around 15 of the U.S.−made C−130 aircraft in operation, all acquired before the 1979 Islamic revolution. Since then, Iran has been subject to tough U.S. sanctions, hindering the purchase of critical spare parts for all

U.S.−made planes in its air force and the civilian flag carrier Iran Air.
Source: http://www.usatoday.com/news/world/2005−12−06−tehrancrash_x. htm

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer